UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,895	02/28/2002	Ted Christian Johnson	10017900-1	2863

7590 10/12/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
PEARSON, DAVID J	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/085,895	**Applicant(s)** JOHNSON, TED CHRISTIAN	
	Examiner David J. Pearson	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claims 21-22 have been amended. Claims 1-28 have been examined.

Response to Arguments

2. Applicant's arguments filed 08/15/2006 have been fully considered but they are not persuasive.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. Claims 1-2, 4, 8 and 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al. (U.S. Patent 6,374,359), and further in view of Rail (Patent Application Publication 2003/0110399), Serbinis et al. (U.S. Patent 6,314,425) and Garrison (U.S. Patent 6,275,939).

For claim 1, Shrader et al. teach a method for authenticating a web session comprising:

receiving a user ID (note column 5, lines 44-50);

encrypting a message using an encryption key (note column 7, lines 21-23); and

converting the encrypted message into an ASCII string (note column 7, lines 33-36).

Shrader et al. differ from the claimed invention in that they fail to specify: computing a message digest of the user ID.

Rail teaches computing a message digest of the user ID (note paragraph [0036]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the device of Shrader et al. with the message digest of Rail to form a system that received a user ID and then created a message digest of the user ID. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al. and Rail because the message digest would provide integrity (note paragraph [0031] of Rail).

The combination of Shrader et al. and Rail differ from the claimed invention in that the fail to specify computing an expiration timestamp for the session and combining the message digest and expiration timestamp.

Serbinis et al. teach computing an expiration timestamp for the session and combining the message digest and expiration timestamp (note column 21, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al. and Rail with the expiration timestamp of Serbinis et al. to from a device which received a user ID, generated a message digest of the ID and computed an expiration timestamp for the session. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail and Serbinis et al. because an expiration timestamp would limit the re-use of a stolen message digest.

The combination of Shrader et al., Rail and Serbinis et al. differ from the claimed invention in that they fail to specify:

selecting an index number;

accessing an encryption key using the index number; and

encrypting the message using the accessed encryption key.

Garrison teaches:

selecting an index number (note column 6, lines 33-36);

accessing an encryption key using the index number (note column 6, lines 33-36); and

encrypting the message using the accessed encryption key (note column 5, lines 61-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al., Rail and Serbinis et al. with the encryption key selection method of Garrison to form a device which performs the steps of the combination of Shrader et al., Rail and Serbinis et al. which selects an index number, selects an encryption key and uses the key to encrypt the combined message digest and expiration timestamp. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Serbinis et al. and Garrison because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack (note column 6, lines 15-22 of Garrison).

For claim 2, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 1, wherein the step of combining the message digest and expiration timestamp more specifically includes concatenating the message digest and expiration timestamp (note column 21, lines 2-4 of Serbinis et al.).

For claim 4, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 1, wherein the step of receiving the user ID more specifically comprises receiving the user ID through an HTML page (note column 5, lines 44-47 of Shrader et al.) that is communicated from a remote client browser (note paragraph [0021] of Rail).

For claim 8, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 1, wherein the step of accessing the encryption key more specifically comprises retrieving an encryption key from a storage segment containing a plurality of encryption keys (note column 6, lines 32-36 of Garrison), wherein the retrieved encryption key is obtained from a location or position within the storage segment based upon the index number (note column 6, lines 32-36 of Garrison).

For claim 11, examiner takes Official Notice that the encrypted message is converted into an ASCII string using a "printf" command ("printf" is a common and easy to implement command which is part of several programming languages, including the C programming language).

For claim 12, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value (note column 6, lines 43-47 and FIG. 7 of Shrader et al.).

4. Claims 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al. (U.S. Patent 6,374,359), and further in view of Rail (Patent Application Publication 2003/0110399), Serbinis et al. (U.S. Patent 6,314,425) and Garrison (U.S. Patent 6,275,939).

For claim 17, Shrader et al. teach a system for authenticating a web session comprising:

Logic configured to receive a user ID (note column 5, lines 44-50);

Logic configured to encrypt a message using an encryption key (note column 7, lines 21-23); and

Logic configured to convert the encrypted message into an ASCII string (note column 7, lines 33-36).

Shrader et al. differ from the claimed invention in that they fail to specify:

logic configured to compute a message digest of the user ID.

Rail teaches logic configured to compute a message digest of the user ID (note paragraph [0036]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the device of Shrader et al. with the message digest of Rail to form a system that received a user ID and then created a message digest of the user ID. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al. and Rail because the message digest would provide integrity (note paragraph [0031] of Rail).

The combination of Shrader et al. and Rail differ from the claimed invention in that the fail to specify logic configured to compute an expiration timestamp for the session and logic configured to combine the message digest and expiration timestamp.

Serbinis et al. teach logic configured to compute an expiration timestamp for the session and logic configured to combine the message digest and expiration timestamp (note column 21, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al. and Rail with the expiration timestamp of Serbinis et al. to from a device which received a user ID, generated a message digest of the ID and computed an expiration timestamp for the session. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail and Serbinis et al. because an expiration timestamp would limit the re-use of a stolen message digest.

The combination of Shrader et al., Rail and Serbinis et al. differ from the claimed invention in that they fail to specify:

Logic configured to select an index number;

Logic configured to access an encryption key using the index number; and

Logic configured to encrypt the message using the accessed encryption key.

Garrison teaches:

Logic configured to select an index number (note column 6, lines 33-36);

Logic configured to access an encryption key using the index number (note column 6, lines 33-36); and

Logic configured to encrypt the message using the accessed encryption key (note column 5, lines 61-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al., Rail and Serbinis et al. with the encryption key selection method of Garrison to form a device which performs the steps of the combination of Shrader et al., Rail and Serbinis et al. which selects an index number, selects an encryption key and uses the key to encrypt the combined message digest and expiration timestamp. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Serbinis et al. and

Garrison because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack (note column 6, lines 15-22 of Garrison).

For claim 18, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach the system of claim 17, further including a system to generate an expiration timestamp (note column 21, lines 1-10 of Serbinis et al.).

For claim 19, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach the system of claims 17, further including logic configured to communicate the ASCII string to a remote computer (note column 7, lines 33-36 of Shrader et al.).

For claim 20, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach the system of claim 17, further including a local memory for storing the plurality of encryption keys (note column 6, lines 32-36 of Garrison).

5. Claim 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al. (U.S. Patent 6,374,359), and further in view of Rail (Patent Application Publication 2003/0110399), Serbinis et al. (U.S. Patent 6,314,425) and Garrison (U.S. Patent 6,275,939).

For claim 21, Shrader et al. teach a method for authenticating a transaction comprising:

encrypting a message using an encryption key (note column 7, lines 21-23); and

converting the encrypted message into an ASCII string (note column 7, lines 33-36).

Shrader et al. differ from the claimed invention in that they fail to specify: computing a message digest of a user ID.

Rail teaches computing a message digest of a user ID (note paragraph [0036]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the device of Shrader et al. with the message digest of Rail to form a system that creates a message digest of the user ID. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al. and Rail because the message digest would provide integrity (note paragraph [0031] of Rail).

The combination of Shrader et al. and Rail from the claimed invention in that the fail to specify:

concatenating the message digest with an expiration timestamp,

Serbinis et al. teach **concatenating the message digest with an expiration timestamp** (note column 21, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al. and Rail with the expiration timestamp of Serbinis et al. to from a device which generated a message digest of the ID, computed an expiration timestamp for the session and concatenated the two. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail and Serbinis et al. because an expiration timestamp would limit the re-use of a stolen message digest.

The combination of Shrader et al., Rail and Serbinis et al. differ from the claimed invention in that they fail to specify:

selecting an index number;

selecting an encryption key from a plurality of encryption keys using the index number; and

encrypting the message using the accessed encryption key.

Garrison teaches:

selecting an index number (note column 6, lines 33-36);

selecting an encryption key from a plurality of encryption keys using the index number (note column 6, lines 33-36); and

encrypting the message using the accessed encryption key (note column 5, lines 61-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al., Rail and Serbinis et al. with the encryption key selection method of Garrison to form a device which performs the steps of the combination of Shrader et al., Rail and Serbinis et al. which selects an index number, selects an encryption key and uses the key to encrypt the message digest. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Serbinis et al. and Garrison because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack (note column 6, lines 15-22 of Garrison).

For claim 22, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 21, wherein the step of encrypting the message more specifically includes encrypting the concatenated message using the accessed encryption key (note column 21, lines 1-10 of Serbinis et al.).

For claim 23, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 21, wherein the step of selecting the encryption key more specifically includes retrieving the encryption key from a local memory based on the index number (note column 6, lines 32-36 of Garrison).

For claim 24, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 21, further includes the step of communicating the ASCII string to a remote computer (note column 7, lines 33-36 of Shrader et al.).

6. Claims 3, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Serbinis et al. and Garrison as applied to claim 1 above, and further in view of Berners-Lee et al. and Verio.

For claim 3, the combination of Shrader et al., Rail, Serbinis et al. and Garrison teach a method of claim 1, further comprising passing the ASCII string to a remote computer using FTP (note paragraph [0021] of Rail) within an HTML page (note paragraph [0024]) of Rail).

The combination of Shrader et al., Rail, Serbinis et al. and Garrison differ from the claimed invention in that they fail to specify the ASCII string is passed in an FTP URL being of the form ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

Berners-Lee et al. teach "URL schemes that involve the direct use of an IP-based protocol to a specified host on the Internet use a common syntax for the scheme-specific data: //<user>:<password>@<host>:<port>/<url-path>" They go on to specify that <user> and <password> as "user: An optional user name. Some schemes (e.g., ftp) allow the specification of a user name. Password: An optional password. If present, it follows the user name separated from it by a colon." (note section 3.1 on page 5)

The Verio glossary defines password as "A series of characters that enables someone to access a file, computer or program." This definition would make the ASCII value a password because it is a series of characters that are enabling a user to access files on an FTP server.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of combination of Shrader et al., Rail, Serbinis et al. and Garrison with passing the ASCII value in an FTP URL of Berners-Lee et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al, Rail, Serbinis et al., Garrison and Berners-Lee et al. because it would provide a convenient way for a user to pass their user ID and password to a FTP server.

For claim 14, the combination of Shrader et al., Rail, Serbinis et al., Garrison and Berners-Lee et al. teach a method of claim 3, further including the step of passing the index number to the remote computer (note column 6, lines 32-36 of Garrison).

For claim 15, the combination of Shrader et al., Rail, Serbinis et al., Garrison and Berners-Lee et al. teach a method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string (note column 6, lines 32-36 of Garrison).

7. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Serbinis et al. and Garrison as applied to claim 1 above, and further in view of Jenkins.

For claim 5, the combination of Shrader et al., Rail, Serbinis et al. and Garrison differ from claimed invention in that they fail to specify the message digest of the user ID more specifically comprises computing a four-byte binary value.

Jenkins teaches a hashing function that "Returns a 32-bit value." (note first paragraph of page 2) Note that a four bytes value is equal to 32 bits.

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al. and Garrison that used the four byte hashing function of Jenkins to create the user ID message digest. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al, Rail, Serbinis et al, Garrison and Jenkins because Jenkins teaches his hash function is "faster and more thorough than the one you are using now." (note Abstract of Jenkins)

8. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Serbinis et al. and Garrison as applied to claim 1 above, and further in view of Krishnaswamy et al (U.S. Patent 6,909,708).

For claim 6, the combination of Shrader et al., Rail, Serbinis et al. and Garrison differ from claimed invention in that they fail to specify the expiration timestamp is computed in Epoch format.

Krishnaswamy et al. teach a communication method that "records timepoints in the epoch time format." (note column 265, lines 37-46)

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al. and Garrison that computed the timestamp in Epoch format of Krishnaswamy et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Serbinis et al., Garrison and Krishnaswamy et al. because it would solve the problems associated with converting to and from daylight savings time (note column 265, lines 37-46 of Krishnaswamy et al.).

9. Claims 7, 10 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Serbinis et al. and Garrison as applied to claim 1 above, and further in view of Tan (U.S. Patent 6,490,353).

For claim 7, the combination of Shrader et al., Rail, Serbinis et al. and Garrison differs from the claimed invention in that they fail to specify the index number used to access the encryption key is randomly generated.

Tan teaches a key management scheme where "it may select these [key start points and lengths] by randomly selecting table entry numbers."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al. and Garrison with the randomly selected index numbers of Tan. One of ordinary skill in the art at the time of the invention would have motivated to combined Shrader et al., Rail, Serbinis et al., Garrison and Tan because an unpredictable sequence of encryption keys would decrease the likelihood of breaking the encryption method.

For claim 10, the combination of Shrader et al., Rail, Serbinis et al. and Garrison differs from the claimed invention in that they fail to specify the step of concatenating the index number to the encrypted message.

Tan teaches a key management scheme where "the seed (randomly generated index number) may be communicated as part of the message transmission."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al. and Garrison which included the index number in the message transmission as taught by Tan. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al, Rail, Serbinis et al., Garrison and Tan because it provide a convenient way of storing the index number so the server would not have to locally store which cookie is encrypted with which key.

For claim 13, examiner takes Official Notice that the encrypted message and the index number are converted into an ASCII string using a "printf" command ("printf" is a common and easy to implement command which is part of several programming languages, including the C programming language).

10. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Serbinis et al. and Garrison as applied to claim 1 above, and further in view of Jenkins and Krishnaswamy et al.

The combination of Shrader et al., Rail, Serbinis et al. and Garrison differs from the claimed invention in that they fail to specify the encrypted combined message digest and timestamp are an eight-byte binary value.

Jenkins teaches a hashing function that "Returns a 32-bit value." Note that a four bytes value is equal to 32 bits.

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al. and Garrison. that used the four byte hashing function of Jenkins to create the user ID message digest because Rail teaches to use "a suitable hashing function" (note paragraph [0027] of Rail) and Jenkins teaches his hash function is "faster and more thorough than the one you are using now." (note Abstract of Jenkins)

The combination of Shrader et al., Rail, Serbinis et al., Garrison and Jenkins differs from the claimed invention in that they fail to specify the encrypted combined message digest and timestamp are an eight-byte binary value.

Krishnaswamy et al. teach an epoch timestamp that is stored in 16 bits. (note column 383, Word 5 of Krishnaswamy et al.)

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al., Garrison and Jenkins that computed the timestamp in Epoch format of Krishnaswamy et al. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Serbinis et al., Garrison and Krishnaswamy et al. because it would solve the problems associated with converting to and from daylight savings time (note column 265, lines 37-46 of Krishnaswamy et al.).

Note using the DES encryption algorithm (note column 5, 61-65 of Garrison) would result in an eight byte binary value. Note, because of the block encryption properties of DES, an input of 48 bits (32 bit hash plus 16 bit timestamp) would result in a one-block output of 64 bits or eight bytes.

11. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Garrison as applied to claim 21 above, and further in view of Swartz et al (U.S. Patent 6,095,418).

For claim 25, the combination of Shrader et al., Rail and Garrison differs from the claimed invention in that it fails to specify including the step of communicating the ASCII string to a person through voice communication.

Swartz et al. teach communicating the ASCII string to a person through voice communication (note column 4, lines 39-44).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Shrader et al., Rail and Garrison with the spoken ASCII of Swartz et al. to form a device which converted the message digest to ASCII and then read the string aloud to someone. One of ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al, Rail, Garrison and Swartz et al. because it provide a convenient way to give the user their authenticated message digest when they do not have access to a computer or an Internet connection.

12. Claims 26-28 rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail and Garrison as applied to claim 21 above, and further in view of Stern (U.S. Patent 6,110,044).

For claims 26-28, the combination of Shrader et al., Rail and Garrison differs from the claimed invention in that they fail to specify the ASCII string is printed onto a ticket selected from the group consisting of an airline ticket, a concert ticket, an employee ID card, and an event ticket and further specifying the ASCII string be printed on the ticket in a form that it may be later electronically scanned for verification.

Stern teaches a ticket printing and verification method which "contains a barcode printer (or other means for embodying a machine-readable indicium in a payout ticket), which prints both alphanumeric and barcode information on a payout ticket, including a validation number." (note column 3, lines 8-12) Note that in this case, a payout ticket would be an event ticket because successful verification of the ticket results in a payout event. Stern also teaches, "Selection circuitry 105 may also contain circuitry for encrypting all or part of the barcoded data imprinted on the payout ticket." (note column 4, lines 49-51)

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail and Garrison, which printed the ASCII string on an event ticket with a bar code of Stern. One or ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Garrison and Stern because it would provide a convenient and secure way to produce and verify the authenticity of a monetary winnings event ticket, which would be ideal for casino or other gaming companies.

13. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shrader et al., Rail, Serbinis et al., Garrison and Berners-Lee et al. as applied to claim 14 above, and further in view of Tan.

For claim 16, the combination of Shrader et al., Rail, Serbinis et al., Garrison and Berners-Lee et al. differs from the claimed invention in that they fail to specify converting the encrypted message into an ASCII string more specifically comprises converting a combination of the encrypted message and the index number into an ASCII string, wherein the index number is communicated to the remote computer as a part of the ASCII string.

Tan teaches a key management scheme where "the seed (randomly generated index number) may be communicated as part of the message transmission."

It would have been obvious to one of ordinary skill in the art at the time of the invention to form the combination of Shrader et al., Rail, Serbinis et al., Garrison and Berners-Lee et al. which includes the index number in the message transmission of Tan. One or ordinary skill in the art at the time of the invention would have been motivated to combine Shrader et al., Rail, Serbinis et al, Garrison, Berners-Lee et al.

and Tan because it would provide a convenient way of storing the index number so the server would not have to locally store which cookie is encrypted with which key.

Response to Arguments

14. Applicant argues the combination of Shrader, Rail, Serbinis and Garrison fail to teach the claim 1 limitation “combining the message digest and expiration timestamp” because the message digest of the instant application is based on a user ID and Serbinis teaches a unique string that is independent of user information (note page 8 of Remarks). Applicant also argues there is no motivation to combine Serbinis with Shrader, Rail and Garrison because of this teaching of an access token independent of user information (note page 9 of Remarks).

Examiner disagrees. Serbinis teaches concatenating an expiry timestamp to a value. In the combination of Shrader, Rail, Serbinis and Garrison, the value Serbinis' expiry timestamp is concatenated with is message digest based on a user ID (as taught by Rail in paragraph [0036]). Additionally, Serbinis teaches using the expiry timestamp to authentication the presented token (note column 21, lines 40-42 of Serbinis et al.). Therefore there is motivation to combine Shrader and Rail with Serbinis because it adds an additionally layer of security which protects against replay attacks.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David J. Pearson whose telephone number is (571) 272-0711. The examiner can normally be reached on Monday - Friday, 8:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER